DPNC GLOBAL

RISK ADVISORY UPDATE

UPI FRAUD: ONLINE PAYMENT FRAUDS SURGING IN THE CAPITAL

Unified Payments Interface (UPI) has transformed the way we handle financial transactions in India. It's fast, easy and convenient, allowing users to make payments and transfers directly from their smartphones. However, with the increase in UPI usage, there has also been a troubling rise in online payment fraud, especially in major cities like Delhi, Chennai, Bangalore, Kolkata etc.

As fraudsters get more sophisticated in their methods, it’s important to take a closer look at how this affects both users and businesses and what auditors can do to help reduce the risks.

Here are some of the most common UPI frauds happening: -

1. **Phishing Scams**: Fraudsters impersonate banks or payment apps, sending fake messages or emails asking users to share their UPI details or OTPs.

2. **SIM Swap Frauds**: Cybercriminals trick mobile network providers into transferring a victim’s phone number to a new SIM card. Once they have access to the phone number, they can reset UPI credentials and steal money.

3. **Fake Payment Links**: Fraudsters send fake payment links through social media, SMS, or email, which lead victims to fake websites or apps that steal their UPI credentials.

4. **QR Code Scams**: Fraudsters create fake QR codes that, when scanned, either steal money or install malicious software on the user’s phone.

While these scams affect individual users, the broader impact on businesses and financial institutions is even more significant, as they may face reputational damage, customer trust issues and regulatory scrutiny.

Why UPI Frauds Happen: Key Vulnerabilities

UPI frauds reveal several vulnerabilities in the system:

1. **Lack of User Awareness**: Many users are still unaware of basic security practices, such as verifying payment requests and being cautious of unknown links or messages.

2. **Weak Fraud Detection Systems**: While banks and payment apps have some fraud detection mechanisms, they may not be sophisticated enough to catch new or evolving fraud tactics in real time.

3. **Insufficient Authentication**: UPI transactions typically require a 6-digit PIN, but this may not be enough protection. Fraudsters use social engineering tactics to trick users into sharing their PINs.

4. **Non-compliance with Security Guidelines**: Some businesses, particularly small merchants and third-party providers, may not follow security best practices, leaving gaps that fraudsters can exploit.

What Auditors Can Do to Address UPI Fraud Risks

Auditors play a critical role in identifying and minimizing the risks associated with UPI fraud. By evaluating an organization's financial systems, auditors can ensure that the right controls and processes are in place to prevent fraud.

Here are some ways auditors can help:

1. **Risk Assessment and Control Evaluation**: Auditors need to assess the overall risk of fraud in UPI transactions. This includes checking the security measures used by financial institutions, reviewing internal controls around UPI payments, and evaluating the authentication processes in place.

   Internal controls should also be tested to make sure they can detect unusual transactions, like large payments, transactions from unrecognized devices, or multiple payments in a short time.

2. **Strengthening Fraud Prevention Measures**: Auditors can ensure that businesses have implemented strong fraud prevention systems, such as multifactor authentication (MFA) for higher-value transactions or sensitive financial activities.

   Encryption should be used to protect payment data, and businesses should perform regular security checks to identify weaknesses before fraudsters can exploit them.

3. **User Education and Awareness:** Since a lot of UPI frauds rely on tricking users, auditors can work with organizations to develop training programs that help customers recognize phishing attempts, fake payment links, and other common scams.

   Regular communication to customers about security practices (e.g., “Don’t share your OTP with anyone” or “Check the payment link before making any transfer”) is essential.

4. **Transaction Monitoring:** Auditors can recommend the implementation of real-time monitoring systems that automatically flag suspicious or unusual transactions. This could include payments made outside normal business hours or from locations that seem unusual for the customer.

   Immediate alerts can help prevent fraud before large sums of money are transferred.

5. **Post Fraud Investigation**: If a fraud incident does occur, auditors must investigate how it happened. They should work with the company and possibly law enforcement to understand whether the fraud was caused by a system vulnerability or a user error, and recommend improvements to prevent it from happening again.

   Regular audits should include reviews of all fraud cases, even minor ones, to identify trends or weaknesses in the system.

Best Practices for Businesses to Prevent UPI Fraud

For businesses that use UPI for payments, taking the right steps to protect their systems and customers is critical. Here are some best practices:

1. **Educate Customers**: Businesses should make sure their customers know how to protect themselves. This can be done through email campaigns, SMS alerts, or even in-app messages.

2. **Use Stronger Authentication Methods**: In addition to UPI PINs, businesses can consider implementing Multi-Factor Authentication (MFA) for all transactions, especially for high-value payments.

3. **Regular Monitor Transactions**: Businesses should set up systems to quickly track and analyze transactions in real time to spot any suspicious behavior.

4. **Comply with Security Guidelines**: It's essential that businesses follow the security measures and standards set by regulators like the Reserve Bank of India (RBI) and the National Payments Corporation of India (NPCI) to ensure compliance and minimize fraud risks.

Conclusion

While UPI has made digital payments more convenient, the rise in frauds is a significant concern. Auditors, businesses, and users all have an important role to play in preventing these scams. Auditors can help by assessing risks, strengthening security controls, and promoting user education to reduce the likelihood of fraud.

For businesses, implementing the right fraud prevention measures, educating customers, and staying updated on security standards can go a long way in safeguarding against UPI fraud. With the right controls in place, we can continue to enjoy the benefits of UPI without falling victim to digital fraud.

By taking proactive steps, we can ensure that UPI remains a safe and trusted payment option for everyone.

Disclaimer

The information contained herein is prepared based on the information available on the public domains. While the information is believed to be accurate to the best of our knowledge, we do not make any representations or warranties, express or implied, as to the accuracy or completeness of this information. Reader should conduct and rely upon their own examination and analysis and are advised to seek their own professional advice. We accept no responsibility for any errors it may contain, whether caused by negligence or otherwise or for any loss, howsoever caused or sustained, by the person who relies upon it.

CONTACT US

NOIDA OFFICE

DPNC GLOBAL LLP

📍 Windsor Grand, 15th Floor,
Plot No. 1C, Sector-126,
Noida-201303, Uttar Pradesh

GURGAON OFFICE

DPNC GLOBAL LLP

120, Vipul Business Park,
Sector-48, Sohna Road,
Gurugram, Haryana-122018

☎ +91.120.6456990

✉ dpnc@dpncglobal.com

🌐 https://dpncglobal.com/

FOLLOW US ON